

Smart DLP



Data Leak Prevention is available from 19.2 and later

Data Leak Prevention is available for the Enterprise editions of FileCloud. Read more about [differences in features between editions](#).



DLP crawlers run on all daily cron jobs and remove shares that violate any SHARE ENFORCE rules.

- [Overview](#)
- [More Information:](#)
 - [Enforce data protection in FileCloud with Smart DLP](#)

Overview

Due to increasing privacy requirements, it is important for organizations to be able to monitor neglectful or malicious activity that can result in the loss of confidential data. The data leak or loss can occur at end points due to user actions, during transit, or while at rest. Data at rest leak prevention relies on encryption technologies and physical security of media, whereas endpoint leak prevention refers to the ability to prevent data leak from an application's end point (e.g. the recipient of a data transfer).

Data leak prevention (DLP) is a FileCloud feature that enables administrators to closely control the degree to which users can access, edit, download, and transfer their organization's files and folders. While DLP can be useful for many different kinds of data, it can be especially critical for the secure handling of Personal Identification Information (PII), Personal Health Information (PHI), and Payment Card Information (PCI). DLP also offers greater security to organizations that are required to operate in compliance with HIPAA or [GDPR](#).

[Smart Classification](#) works in conjunction with DLP to streamline, automate, and strengthen data security.

More Information:

FileCloud Videos	FileCloud Blogs
	<ul style="list-style-type: none">• Enforce data protection in FileCloud with Smart DLP

In this section

- [Creating Data Leak Prevention Rules](#)
- [Example Rules](#)
- [Rule Expressions](#)
- [Metadata, Smart Classification, and Smart DLP](#)
- [How to secure documents with Smart DLP & CCE](#)